THABACHWEU LOCAL MUNICIPALITY

Acceptable Use

Policy

The Thabachweu Local Municipality's intentions for publishing policies and procedures is not to impose restrictions that are contrary to the Municipality's established culture of openness, trust and integrity. The Municipality is committed to protecting its employees, clients, and service providers from any illegal or damaging actions by individuals, either knowingly or unknowingly.

Thabachweu Local Municipality

Table of Contents

1. Overview

The Thabachweu Local Municipality's intentions for publishing an Acceptable use policy is not to impose restrictions that are contrary to the Municipality's established culture of openness, trust and integrity. The Municipality is committed to protecting its employees, clients, and service providers from any illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet related systems, including computer equipment, software, operating systems, storage media, mail accounts, internet browsing, and FTP uploads, are the sole property of the Thabachweu Local Municipality. These systems are to be used for business purposes and serving the best interests of the Municipality, that of its clients and service providers.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and /or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the Municipality and to protect its employees. Inappropriate use will expose the Municipality and it's users to risks including virus attacks and malicious code to compromise network systems and shared services.

3. Scope

This policy applies to all the Thabachweu Local Municipality employees, contractors, consultants, service providers, and any other workers at the Municipality, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Municipality

4. Policy

4.1. General Use and Ownership

- The Thabachweu Local Municipality Security Officer desires to provide a reasonable level of privacy therefore users should take note that the data they create and store on the Municipality's IT infrastructure remains the property of the Thabachweu Local Municipality.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of municipal systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

- Before any information that users consider sensitive or vulnerable are encrypted written approval must be obtained from the Municipality's Security Officer
- The Security Officer may at any given date or time authorized certain IT individuals or service providers to monitor equipment, systems and network traffic for maintenance and support purposes.
- Mail Attachment Size Limits are determined by the external mail service provider.
    - Mailbox size 100mb
    - Maximum mail message size 10mb
    - Number of recipients 100

4.2. Security and proprietary information

- The user interface for information contained on Internet / Intranet / Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K/XP users) when the host will be unattended.
- Pre-approval must be obtained from the Municipality's Security Officer before confidential files are encrypted.
- Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
- Postings by employees from the Municipality's email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Thabachweu Local Municipality, unless posting is in the course of business duties.
- All hosts used by the employee that are connected to the Municipality's network or internet system, whether owned by the employee or the Municipality, shall be continually executing approved virus-scanning software with a current virus signature.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration

staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the Thabachweu Local Municipality authorized to engage in any activity that is illegal under local, governmental or international law while utilizing the Municipality's - owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

5. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for the Thabachweu Local Municipality.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Thabachweu Local Municipality end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using the Municipality's computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Thabachweu Local Municipality account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program, script, command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet.
- Providing confidential information about the Municipality, or its employees to parties outside the Thabachweu Network.

6. E-mail and communication activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within the Municipality's networks of other Internet, Intranet, Extranet service providers on behalf of, or to advertise, any service hosted by the Municipality or connected via the Municipality's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Acceptable mail data transfer per month per user should not exceed
    - 500Mb for mail sending and 500Mb for mail receiving
    - Combined mail sending and receiving should not exceed 1000Mb (1Gb)
    - Attachments should not exceed 5Mb.
- A maximum of 50 recipients per mail message are allowed

7. Corrective actions for non-policy compliance

- Failure to comply with the guidelines stipulated in the Municipality's policies will result in the following corrective or disciplinary procedures.
- The decisive action that will be taken against the employee is dependent on the severity level and the level of the security risk.
- Warning from Management
    - The employee receives a warning from their manager that they were in violation of policy.
- Written Warning in Personnel File

- The employee is reprimanded, and official notice is put in their personnel file. This may have negative consequences during future performance reviews or promotion considerations.

- Revoking Privileges
  - Access to certain resources, such as internet or email, can be revoked for a limited period providing that this action does not have a negative impact on the employee's job functions.
- Training
  - Adequate training to create awareness and guidance on policy compliance.
- Disciplinary action will be determined in compliance to Schedule 8 of the Labour Relations Act 66 of 1995 or other related Public Service Regulations.

8. Glossary and Abbreviations

Please refer to the Thabachweu Glossary and abbreviations guide.

Version Control

Version	State/Change	Author	Date
1.0	Original	Sbusiso Langa	
1.1	Changes	Sbusiso Langa	

Author

Name	Designation	Signature	Contact
Sbusiso Langa	Security Officer		+27 13 235 7367

Review

Name	Designation	signature	Date

Approval

Name	**Designation**	**Signature**	**Date**